UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,615	07/30/2001	Phillip W. Rogaway	ROG01-0002	3083

22835 7590 08/23/2005

A. RICHARD PARK, REG. NO. 41241
PARK, VAUGHAN & FLEMING LLP
2820 FIFTH STREET
DAVIS, CA 95616

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 08/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/918,615	ROGAWAY, PHILLIP W.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *67-70* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *68* is/are allowed.

6)☒ Claim(s) *67,69-70* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 July 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 67-70 have been considered.

Specification

The abstract is objected to for being too long. The abstract should be revised and follow the guidelines below.

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

Drawings

Figures 6-10 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Allowable Subject Matter

The following is a statement of reasons for the indication of allowable subject matter: Claims 67-68 present an authenticated-encryption method which distinguishes over the prior art. Though the idea of an authenticated-encryption method is known in the prior art and has been done by inventors such as

Gligor, the examiner finds no mention of the following claim limitation used in an authenticated-encryption method:

"using the block cipher, the key, and the nonce to generate a sequence of m offsets, each offset having n bits, wherein the sequence of offsets is computed by (a) computing a 0^{th} basis offset by applying the block cipher, keyed by the key, to a constant; (b) for each positive number i, defining the ith basis offset from the prior basis offset by shifting the prior basis offset left one position, and then xoring the resulting value with a constant that depends on the first bit of the prior basis offset; (d) computing a base offset by applying the block cipher, keyed by the key, to the xor of the 0^{th} basis offset and the nonce; (e) defining the 1^{st} offset in the sequence of offsets as the xor of the 0^{th} basis offset and the base offset; and (f) for each integer i between two and m, defining the ith offset in the sequence of offsets as the xor of the prior offset and the jth basis offset, where j is the number of zero-bits following the last one-bit when the number is written in binary".

Furthermore, the examiner does not believe the specific claim limitation above would have been obvious to one of ordinary skill in the art at the time the invention was filed as the limitation is integrally used in the system to form a cohesive approach to performing an efficient authenticated-encryption method.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 67 and 69 are directed to non-statutory subject matter. The claims are directed to an abstract method which requires nothing tangible. The examiner suggests the applicant amend the preamble to "A computer-implemented authenticated-encryption method" from "An authenticated-encryption method". Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 69-70 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gligor, U.S. Patent No. 2001/0033656, in view of Jutla (Jutla, Charanjit. Encryption Modes with Almost Free Message Integrity. August 2000) in further view of Menezes (Menezes, Alfred J. Handbook of Applied Cryptography. 1997. CRC Press. Pages 321-383).

As per claims 69-70, the applicant describes an authenticated-encryption method that uses an n-bit block cipher, a key, and an n-bit nonce to encrypt a message into a ciphertext, the method comprising the following limitations which are met by Gligor, Jutla, and Menezes:

a) partitioning the message into m-1 message blocks and one final fragment, each message block having n bits and the final fragment having between 0 and n bits (Gligor: Fig 9);

b) generating m+1 offsets using a sequence shift and xor operations, this sequence of shift and xor operations being applied to a starting value determined using the block cipher, the key, and the nonce (Gligor: Fig 9);

c) for each number i between 1 and m-1, xoring the ith message block with the ith offset to determine an ith input block (Jutla: Fig 2 of page 5);

d) for each number i between 1 and m-1, applying the block cipher, keyed by the key, to the ith input block, to determine an ith output block (Jutla: Fig 2 of page 5);

e) for each number i between 1 and m-1, xoring the ith output block with the ith offset to determine an ith ciphertext block (Jutla: Fig 2 of page 5);

f) concatenating the m-1 ciphertext blocks to determine a ciphertext body (Gligor: Fig 9);

g) computing an encoded length by encoding the length of the final fragment as an n-bit string (Jutla: [0025]);

h) xoring the encoded length with the mth offset to determine a precursor pad (Menezes: page 340);

i) computing a pad by applying the block cipher, keyed by the key, to the precursor pad (Gligor: Fig 9);

j) xoring the final fragment with a portion of the pad to determine a ciphertext fragment having the same length as the final fragment (Menezes: page 340);

k) computing a padded ciphertext fragment by appending to the ciphertext fragment a sufficient number of zero bits so that the padded ciphertext fragment has n bits (Gligor: [0025];

l) computing a checksum by xoring together the m-1 message blocks, the pad, and the padded ciphertext fragment (Gligor: Fig 9);

m) computing a precursor full tag by xoring together the checksum and the (m+1)st offset (Gligor: Fig 9);

n) determining a full tag by applying the block cipher, keyed by the key, to the precursor full tag (Gligor: Fig 9);

o) computing a tag as a portion of the full tag (Gligor: Fig 9);

p) defining the ciphertext to be the ciphertext body, the ciphertext fragment, and the tag (Gligor: Fig 9);

Gligor discloses an authentication-encryption technique which meets most of the limitations of the above claim. However, Gligor does not disclose that an offset is combined with a message block before the block cipher. Jutla discloses an authenticated-encryption method similar to that of the applicant's called IAPM (Integrity Aware Parallizable Mode). Jutla discloses that an offset (S_i in Fig 2) is combined with a message block before the block cipher. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Jutla with those of Gligor and combine an offset with a message block before the block cipher because doing so incorporates an additional technique to provide further encipherment and thus more security for the data.

Gligor in view of Jutla disclose an authentication-encryption technique which meets most of the limitations of the above claim. However, Gligor in view of Jutla do not disclose that the message fragment is combined with the pad to form the ciphertext fragment and that an offset is combined to form a precursor pad before the block encipherment. Menezes discloses combining the ciphertext fragment with the pad. Menezes discloses a block ciphering method known as Matyas-Meyer-Oseas in which an input message is combined with the result of a block cipher process to form ciphertext. Combining the ideas of Menezes with those of Gligor in view of Jutla would allow x4 to be combined at 92 with z4. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Menezes with those of Gligor in view of Jutla because doing so incorporates an additional technique to provide further encipherment and thus more security for the data.

Conclusion

THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KS

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER